



Department of Homeland Security Daily Open Source Infrastructure Report for 04 June 2007

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](#)

<http://www.dhs.gov/>

Daily Highlights

- American Electric Power, which operates Southwestern Electric Power Company, is reporting a rise in the theft of electrical equipment because the market for scrap metal is driving a drastic increase in the theft of metal — especially aluminum and copper. (See item [4](#))
- The New York Times reports four men, including a onetime airport cargo handler and a former member of the Parliament of Guyana, were charged on Saturday, June 2, with plotting to blow up fuel tanks, terminal buildings, and the fuel lines running beneath John F. Kennedy International Airport. (See item [9](#))

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *June 01, Daily Progress (VA)* — **Fines, rules apply to power grid.** Regulators of the North American power grid soon will gain the authority to issue \$1 million-a-day fines to companies that violate electric reliability rules. Nearly four years after the country's biggest-ever blackout, 83 mandatory standards will take effect. Experts, however, do not expect major fines to result — at least not right away. After the outage August 14, 2003, left tens of millions of people in the dark, federal energy regulators criticized the electricity industry's then-voluntary efforts to ensure power grid reliability, saying the industry played down the grid's shortcomings and used

ambiguous and often-ignored standards. Congress, as part of an energy bill passed in 2005, required that grid operators meet mandatory reliability standards. The regulations were scheduled to go into effect Monday, June 1, but were pushed back until June 18. The delay was caused by an interpretation of law which mandates that federal agencies' rules go into effect 60 days after they are published in the Federal Register. David Hilt of the North American Electric Reliability Corp. said that utilities and other power companies are well on their way toward complying.

Source: http://www.dailyprogress.com/servlet/Satellite?pagename=CDP%2FMSGArticle%2FRTD_BasicArticle&c=MGArticle&cid=1173351432555_&path=!business

2. *June 01, Government Accountability Office* — **GAO-07-676R: Oil and Gas Royalties: A Comparison of the Share of Revenue Received from Oil and Gas Production by the Federal Government and Other Resource Owners (Report).** Amid rising oil and gas prices and reports of record oil industry profits, a number of governments have taken steps to reevaluate and, in some cases, increase the share of oil and gas revenues they receive for the rights to develop oil and gas on their lands and waters. Based on results of a number of studies, the U.S. federal government receives one of the lowest government takes in the world. Collectively, the results of five studies presented in 2006 by various private sector entities show that the United States receives a lower government take from the production of oil in the Gulf of Mexico than do states—such as Colorado, Wyoming, Texas, Oklahoma, California, and Louisiana—and many foreign governments. Other government-take studies issued in 2006 and prior years similarly show that the United States has consistently ranked low in government take compared to other governments.

Abstract: <http://www.gao.gov/docsearch/abstract.php?rptno=GAO-07-676R>

Source: <http://www.gao.gov/docsearch/abstract.php?rptno=GAO-07-676R>

3. *May 31, Research and Markets* — **Report: U.S. has 100 nuclear reactors supplying more than 20 percent of the nation's electricity.** The U.S., France, Germany, Japan, Russia, and South Korea are the largest users of nuclear power. China, India, and Southeast Asia are among regions likely to initiate more rapid adoption of nuclear reactors. Nuclear power is moving to next generation systems that promise to be more efficient and safer than initial systems. Domestically, the United States has 100 nuclear reactors supplying more than 20% of the nation's electricity. Enrichment capacity complements raw material uranium. USEC seeks to provide enrichment capacity. Nuclear power supplies a sixth of world electricity demand. A period of little new construction is ending and the market is at the threshold of significant expansion globally. There are multiple drivers for this upsurge in interest. Over half of the world's production of uranium from mines is in Canada and Australia. After a decade of falling mine production to 1993, output has generally risen and comprises 60 percent of demand for power generation.

Source: <http://www.electricnet.com/content/news/article.asp?DocID={DA917B3C-48D1-4953-B3BD-15BB2453589A}&Bucket=Current+Headlines>

4. *May 31, Shreveport Times (LA)* — **Copper theft a problem for AEP, company says.** American Electric Power, which operates Southwestern Electric Power Company (SWEPCO) in Louisiana, is reporting a rise in the theft of electrical equipment because the market for scrap metal is driving a drastic increase in the theft of metal — especially aluminum and copper, the company said Thursday, May 31. There were seven fatalities last year due to theft and live wire

contacts, including a public fatality in December 2006 in Kilgore, TX, from copper theft. SWEPCO has recently investigated copper theft incidents at company facilities in Longview, Marshall, Gilmer, Gladewater and Mineola, and in Haughton. Some thieves are even cutting into power lines and other equipment that is energized and serving customers. According to Malcolm Smoak of SWEPCO: "A complete wiring system helps provide a safer and more reliable source of electricity...An element of protection is lost when the design of the electric delivery system is altered in an attempt to get at the metal for resale to a salvage center." And, some thieves are getting even bolder, deliberately posing as utility or construction workers. SWEPCO serves more than 464,000 customers in western Arkansas, northwestern Louisiana, and eastern and North Texas.

Source: <http://www.shreveporttimes.com/apps/pbcs.dll/article?AID=/20070531/BREAKINGNEWS/70531031>

5. *May 31, Associated Press* — **Explosives, detonating material stolen from truck in Arkansas.** Bella Vista, AK, police are searching for explosives, blasting caps and detonating cord stolen from four trucks over the weekend. Police say ten tubes of Chempac explosives, the cord and ten blasting caps were taken from the trucks belonging to C & N Electric. Steve King, the electric company's president, says a Chempac tube contains a chemical substance which has to be mixed with another chemical to make it explode. King says workers use the explosives to blow holes for electric poles.

Source: <http://www.wmcstations.com/Global/story.asp?S=6592962>

6. *May 31, Journal News (NY)* — **Massachusetts power plant inadvertently sends alerts to New York.** A Massachusetts nuclear plant's efforts to improve its warning system startled Hudson Valley, NY, emergency officials when a computer accidentally faxed blank radiological advisories to the four counties around Indian Point. The event was quickly determined not to be an actual emergency, but the Nuclear Regulatory Commission (NRC) wants to ensure that the glitch doesn't happen again. Emergency officials at the Pilgrim nuclear plant in Plymouth, MA, run by Indian Point owner Entergy Nuclear Northeast, checked out their sister plant's emergency-alert software about 5 p.m. EDT Tuesday, May 29, to see whether it might work there. Pilgrim officials tried out what they thought was a demonstration version of the software being deployed in the Hudson Valley, Indian Point officials said, but quickly found out that they had Indian Point's actual software when the computer sent emergency faxes to Westchester, Rockland, Putnam and Orange counties as well as to New York state — more than 200 miles away. "They wanted to see if this program would work for them and they pushed the button, but the default settings were for Indian Point," said Neil Sheehan of the NRC. "Guess where the faxes ended up? In the counties surrounding Indian Point."

Source: http://www.nynews.com/apps/pbcs.dll/article?AID=/20070531/NE_WS01/705310387

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report.

[[Return to top](#)]

Banking and Finance Sector

7. *June 01, Security Focus* — **Online thieves nab \$450,000 from town accounts.** A keylogger on the computer of the Carson, CA, treasurer enabled online thieves to transfer nearly half a million dollars to other bank accounts, according to news reports. The thieves made two transfers: The first on May 23 for \$90,000 and the next for \$358,000 on the following day, according to a report in the Los Angeles Times. Carson Treasurer Karen Avilla noticed the transfers on May 24 and, with the help of the town's bank, froze all but \$45,000 of the money. A computer forensics team from the bank found a Trojan horse on her city-issued laptop, according to a report in ComputerWorld. News of online thieves making off with people's data have become commonplace. The theft of funds from companies is far less likely to be reported. A massive breach of retail giant TJX Companies' processing systems led to the loss of information on at least 45.6 million credit and debit cards. The U.S. Secret Service is currently tracking the path of the \$45,000 missing from the accounts.
Source: <http://www.securityfocus.com/brief/514>

8. *May 31, Internal Revenue Service* — **IRS warns of new e-mail scams.** The Internal Revenue Service on Thursday, May 31, alerted taxpayers to the latest versions of an e-mail scam intended to fool people into believing they are under investigation by the agency's Criminal Investigation division. The e-mail purporting to be from IRS Criminal Investigation falsely states that the person is under a criminal probe for submitting a false tax return to the California Franchise Board. The e-mail seeks to entice people to click on a link or open an attachment to learn more information about the complaint against them. The IRS warned people that the e-mail link and attachment is a Trojan Horse that can take over the person's computer hard drive and allow someone to have remote access to the computer. Similar e-mail variations suggest a customer has filed a complaint against a company and the IRS can act as an arbitrator. The latest versions appear aimed at business taxpayers as well as individual taxpayers.
Source: http://www.wane.com/Global/story.asp?S=6593482&nav=menu32_2

[[Return to top](#)]

Transportation and Border Security Sector

9. *June 03, New York Times* — **Four accused of plot to blow up facilities at New York airport.** Four men, including a onetime airport cargo handler and a former member of the Parliament of Guyana, were charged on Saturday, June 2, with plotting to blow up fuel tanks, terminal buildings and the web of fuel lines running beneath John F. Kennedy International Airport. One defendant, the former cargo handler, Russell Defreitas, was arraigned Saturday in federal court in Brooklyn. He is a 63-year-old Guyanese native and naturalized American citizen who lives in Brooklyn. Mark J. Mershon, the assistant director in charge of the Federal Bureau of Investigation field office in New York, said all four men had "fundamentalist Islamic beliefs of

a violent nature,” although they appeared to be acting on their own and had no known connection to al Qaeda. Law enforcement officials said that Kennedy, which handles roughly 45 million passengers a year and 1,000 flights a day, was never in imminent danger because the plot was only in a preliminary phase and the conspirators had yet to lay out detailed plans or obtain financing or explosives. Oil industry experts said safety shut-off valves would almost assuredly have prevented an exploding airport fuel tank from igniting all or even part of the network.

Source: http://www.nytimes.com/2007/06/03/nyregion/03plot.html?_r=1&hp&oref=slogin

10. *June 01, Associated Press* — **Washington State ferry rams dock; one injured.** A passenger ferry rammed the outer dock at the Mukilteo terminal north of Seattle on Friday, June 1, injuring at least one person and damaging the vessel and some pilings. One person had minor injuries after falling down stairs but was not hospitalized, ferry system spokesperson Susan Harris. She said the ferry Cathlamet appeared to have a puncture above the water line and the terminal was temporarily closed. Officials did not immediately know the cause of the accident, Harris said. The Coast Guard is investigating, along with the ferry system. Harris said part of the investigation will include a drug test for the captain. The 328-foot Cathlamet can carry 1,200 passengers and 124 vehicles. Its 21-mile route from Mukilteo to Clinton is heavily used by commuters and weekend travelers to Whidbey Island.

Source: http://hosted.ap.org/dynamic/stories/F/FERRY_ACCIDENT?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

11. *June 01, Newsday (NY)* — **Man wielded box cutter on New York bridge.** A man wielding a box-cutter razor slashed himself repeatedly and threatened to jump off the George Washington Bridge, forcing the closure of the upper deck of the bridge for more than two hours Friday, June 1, creating a massive traffic jam that snarled the New Jersey Turnpike and Cross Bronx Expressway for miles before being apprehended by emergency services officers. A spokesperson for the Port Authority of New York & New Jersey, which operates the bridge, said the man climbed the bridge cable on the north side of the span at 7:06 a.m. EDT and threatened to jump. Armed with a box-cutter razor, police said the man, who has not been identified, slashed his arms and wrists "numerous times" before being talked down off the bridge cable by emergency services officers from a Port Authority special operations tactical unit, as well as emergency services personnel from the New York City Police Department. The closure caused horrendous traffic jams surrounding the bridge, which spans the Hudson River and is the main arterial between New York and New Jersey. Police said their investigation into how the man got onto the bridge is continuing.

Source: <http://www.newsday.com/news/local/longisland/ny-ligeor0602.0.534813.story?coll=ny-top-headlines>

12. *June 01, Tampa Bay Business Journal (FL)* — **Port security upgrades funded, credential program examined.** The Tampa Port Authority has received a \$475,000 seaport grant from the Department of Homeland Security that will be used for enhanced access control, upgrading communications and cameras. The port authority will make a 25 percent match, or about a \$100,000, for the effort. Although the Port of Tampa is set ready for the upgrades, Rep. Kathy Castor, (D-Tampa), introduced an amendment earlier this month concerning the Transportation Worker Identification Credential. The amendment, which the House later passed, requires the Department of Homeland Security to work with Florida, among other states, to resolve

differences between the TWIC and existing access control card programs. Without the amendment, the port would also be required to run two extensive background checks per employee starting in 2008.

Source: <http://tampabay.bizjournals.com/tampabay/stories/2007/05/28/daily41.html>

13. *June 01, BostonChannel* — **Last section of Boston's Big Dig to reopen.** Officials plan to open the last remaining section of the Central Artery tunnel system this weekend that was closed after a fatal ceiling panel collapse. Governor Deval Patrick announced Friday, June 1, that the Interstate 90 East High Occupancy Vehicle tunnel to Logan International Airport will reopen Saturday at about 2 a.m. EDT. The tunnel's ceiling support system underwent a complete review in the wake of the July 2006 accident that claimed the life of Milena Del Valle. Since then, a new bracket and hanger system has been installed to support the concrete panels in the exhaust plenum located below the roof. The process of thoroughly examining, remediating and reinspecting the tunnel's ceiling support system has now been completed," said Transportation and Public Works Secretary Bernard Cohen.

Source: <http://www.thebostonchannel.com/news/13427439/detail.html>

14. *May 31, USA TODAY* — **Travelers face frustrating passport delays.** Swamped by a record number of applications since a January 23 expansion of passport requirements for travelers returning by air from Canada, Mexico, and the Caribbean, the U.S. Department of State is scrambling to keep up. Last week, the department's Website extended its recommended lead time, telling Americans to apply at least 12 weeks before they plan to travel. The department says an expedited passport, which costs an extra \$60 and now accounts for about 50 percent of new applications, takes two to three weeks. But according to several congressional representatives fielding an influx of calls from frantic constituents, wait times can stretch much longer. Ann Barrett, deputy assistant secretary of state for passport services, says the agency is handling 1.5 million applications a month and is on track to issue 17 million new passports this year, an increase of 40 percent from a year ago.

Department of State: <http://travel.state.gov/>

Source: http://www.usatoday.com/travel/news/2007-05-31-passport-woes_N.htm?loc=interstitialskip

15. *May 31, Reuters* — **Leaner Northwest Airlines exits bankruptcy.** Northwest Airlines Corp. exited bankruptcy on Thursday, May 31, marking the end of a 20-month Chapter 11 reorganization and the first time in almost five years that no major U.S. airline is bankrupt. Northwest spent a year-and-a-half hacking \$2.4 billion off its annual costs, mostly from an aggrieved work force. Like other so-called "legacy" carriers in the ailing airline industry, it was forced to slash costs to compete with newer low-cost carriers and deal with wild spikes in fuel costs. The company officially relaunched itself as a slimmed-down carrier with a market value of almost \$7 billion. Northwest's emergence from bankruptcy protection appears to signal the end of a five-year period of turbulence for U.S. airlines, as it and its rivals have made strides toward ensuring their long-term survival. But despite major cost cuts, Northwest faces intense competition, soaring fuel prices and furious employees who resent forfeiting \$1.4 billion annually only to see their bosses net enormous payouts from stock and options awards.

Source: http://biz.yahoo.com/rb/070531/northwest_shares.html?.v=10

[[Return to top](#)]

Postal and Shipping Sector

Nothing to report.

[\[Return to top\]](#)

Agriculture Sector

Nothing to report.

[\[Return to top\]](#)

Food Sector

16. *June 01, CBS News* — Peanut butter salmonella cases now top 600. The number of people sickened since August by peanut butter tainted with salmonella has grown by more than 200. The outbreak, first reported in February, now includes 628 cases in 47 states, the U.S. Centers for Disease Control and Prevention (CDC) said Thursday, May 31. It is the first update on the number of cases linked to the outbreak since early March, when officials said 425 cases had been confirmed in 44 states. ConAgra Foods Inc. recalled all its peanut butter in February after government investigators linked the bacteria outbreak to Peter Pan and Great Value peanut butter. The states with no illnesses reported are Hawaii, New Hampshire and Utah, the CDC said. Wal-Mart has continued selling Great Value peanut butter — its store brand — that is made by different suppliers, but Peter Pan has yet to return to stores.

Source: <http://www.cbsnews.com/stories/2007/06/01/health/main2873807.shtml>

17. *June 01, Reuters* — China goes on offensive after food safety scares. China hit back on Friday, June 1, at accusations its products are unsafe, pointing out that a quarter of imported children's milk bottles and teats failed a recent random quality test in a southeastern province. It was the latest in a spate of reports in China's carefully controlled media lambasting foreign goods for supposed safety and health problems. The products came from Japan, Germany, Britain, Singapore, Thailand, Indonesia, Taiwan and Hong Kong, Xinhua said, adding, "most of them were brand-name goods." This week alone, China has turned away 30 tons of frozen seafood from Australia that it said was tainted with heavy metals, and gave five container loads of Evian mineral water a failing grade for having too many micro-organisms.

Source: <http://www.reuters.com/article/worldNews/idUSPEK9792620070601>

18. *May 30, Associated Press* — South Korea bars beef from U.S. facility. South Korea said Wednesday, May 30, it has suspended beef imports from a U.S. meat processing plant after finding banned bone material in a recent shipment. Seoul prohibited U.S. beef imports in December 2003, after mad cow disease surfaced in the U.S. But the country partially reopened the market last year, on the condition that imports contain only boneless meat from cattle younger than 30 months. However, the first three shipments were turned back for containing tiny bone pieces. It was only last month that a U.S. beef shipment passed quarantine inspections for the first time since imports were resumed. On Wednesday, the Agriculture Ministry said rib bones were found in two boxes of a 15.2-ton shipment. The ministry suspended imports from the U.S. facility that processed the beef in that shipment. The facility, whose name and location

were not released, is one of 36 American plants authorized to process South Korea-bound meat.

Source: <http://www.chron.com/dispatch/story.mpl/ap/fn/4847179.html>

[\[Return to top\]](#)

Water Sector

19. *June 01, KTVU (CA)* — California shuts down bay area water system. State officials stopped the massive pumps that send water to some 25 million Californians and thousands of acres of crop land, a move aimed at protecting an endangered fish in the Sacramento–San Joaquin River Delta. The Harvey O. Banks pumping station outside Tracy was shut down Thursday, May 31, to protect the delta smelt, a small, silvery fish that's considered a key indicator of the delta's health. The voluntary measure was scheduled to last seven to 10 days. The move comes less than two weeks after officials reported the smelt population at an all-time low, raising questions about the species' ability to survive. The three-inch long fish are protected under the California Endangered Species Act. The shutdown follows an April decision by an Alameda County judge ordering the state to stop pumping water out of the delta within 60 days. The judge ruled that the Department of Water Resources lacks the proper permits or authority to run the Banks pumping station, where smelt have been getting trapped. The state has appealed the ruling.

Source: <http://www.ktvu.com/news/13426288/detail.html>

20. *May 30, Minneapolis Star–Tribune* — Chemical detected in nearly 100 private wells. A former 3M chemical that has contaminated municipal wells in six east-metro communities has also been detected in nearly 100 private wells, Minnesota health officials said Wednesday, May 30. Minnesota experts do not know the potential long-term health risks from drinking water that contains PFBA, the chemical in question, but the latest findings are higher than the state's guideline of one part per billion. Virginia Yingling, hydrogeologist for the Minnesota Department of Health, said the wells were among 350 sampled during the past three months after the state found the chemical early this year in the public drinking water of Woodbury, Cottage Grove, St. Paul Park, Hastings, South St. Paul and Newport. Yingling said that the private well results were not surprising and that the source appears to be a 3M disposal in Woodbury that the company used decades ago to bury waste.

Source: <http://www.startribune.com/462/story/1216170.html>

[\[Return to top\]](#)

Public Health Sector

21. *June 01, Thanh Nien (Vietnam)* — Vietnam reports another human bird flu case. A worker at a slaughterhouse in Hanoi, Vietnam, tested positive for the H5N1 virus strain, Nguyen Duc Hien, head of the National Institute for Tropical Diseases, said. He was admitted to the institute May 26, just 12 days after starting to work at the abattoir. Hien said the man was recovering and his condition stable. Director of Hanoi's Bach Mai Hospital, Tran Thuy Hanh, said in the past two days two patients had been admitted with typical bird flu symptoms, one of whom had

died Friday, June 1. Meanwhile, tests have confirmed that all 300 ducklings culled on a farm last Monday in the northern province of Hung Yen had the H5N1 strain of bird flu. The outbreak in Hung Yen brought to 14 the number of areas infected in Vietnam in the past month. They lie from Son La in the country's far northwest to Can Tho city in the Mekong delta in the far south.

Source: <http://www.thanhniennews.com/healthy/?catid=8&newsid=28663>

22. *June 01, Agence France–Presse* — **Indonesian teenager dies of bird flu.** A teenage girl has died of bird flu in Indonesia, taking the death toll in the nation worst hit by the virus to 79, a health ministry official said Friday, June 1. The 15-year-old died on Tuesday, four days after she was admitted to hospital on the main island of Java, the official said. She fell ill after handling and eating a dead chicken at her home in Kendal district in Central Java, said Muhammad Nadirin from the ministry's bird flu information center. "Four out of six chickens at her house died suddenly on May 12. One of the dead chickens was cooked and eaten by the victim," Nadirin said.

Source: http://news.yahoo.com/s/afp/20070601/hl_afp/healthfluindonesia_070601145617;_ylt=AvTem7PH_3UYHRw84pohmxyJOrgF

23. *June 01, Agence France–Presse* — **Hong Kong bird confirmed with H5N1 virus.** A starling has tested positive for the H5N1 bird flu virus in Hong Kong, agricultural officials said Friday, June 1. Authorities said the bird, found dead last week in a densely populated central area, was confirmed with the strain by laboratory tests. It was the 16th wild bird that has been found dead in Hong Kong this year with H5N1, which has killed almost 200 people and ravaged poultry flocks worldwide since 2003.

Source: http://news.yahoo.com/s/afp/20070601/hl_afp/healthfluhongkong_070601161552;_ylt=Av1lOyf.cA_XAD43jQiXyJmJOrgF

24. *May 31, U.S. Food and Drug Administration* — **FDA finalizes guidances for pandemic and seasonal influenza vaccines.** The U.S. Food and Drug Administration (FDA) Thursday, May 31, issued final recommendations to increase the supply of influenza vaccines for both seasonal and pandemic use. FDA's goal with the guidances is to outline the regulatory pathways for the rapid development and approval of these products. In March 2006, FDA issued two draft guidance documents for public comment — one for seasonal influenza vaccines and another for pandemic influenza vaccines. The draft documents outline specific approaches for manufacturers to develop new vaccines that are safe, pure, and potent. The final guidances reflect public input, including vaccine companies and public health officials. Both guidances recommend using recent technologies such as cell culture and recombinant manufacturing to enhance the development and evaluation of vaccines. They also recommend adding substances that improve the immune response from the vaccine (novel adjuvants). The guidance documents represent the FDA's ongoing efforts under its Critical Path Initiative to translate scientific advances, such as cell-culture derived and recombinant vaccine technologies, into new medical products with shorter approval timeframes.

Source: <http://www.fda.gov/bbs/topics/NEWS/2007/NEW01645.html>

[[Return to top](#)]

Government Sector

25. *June 01, Associated Press* — **University of Kansas searched after gunman report.** Police searched buildings at the University of Kansas in Lawrence, on Friday, June 1, after receiving a report of a man with a rifle near the center of campus, but they found nothing suspicious. The caller had reported seeing the man near Wescoe Hall, which houses the school's English Department, university spokesperson Todd Cohen said. The university was not placed on lockdown, but faculty, staff and students were sent an e-mail shortly after 10 a.m. CDT advising them to stay indoors. The search, involving university police and officers from Lawrence and Douglas County, was called off after about an hour, according to a notice on the university's Website.

Source: http://hosted.ap.org/dynamic/stories/U/UNIVERSITY_SEARCHED?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

[\[Return to top\]](#)

Emergency Services Sector

26. *June 01, Department of Homeland Security* — **Hurricane season preparations.** Hurricane season runs from June 1 through November 30. The Federal Emergency Management Agency (FEMA) and the Department of Homeland Security (DHS) have been working closely with state and local governments and relief organizations to remind residents and businesses in coastal areas to make emergency preparations. There is no substitute for individual preparedness when it comes to the safety of individuals and their families. By taking small steps, those who can make preparations allow local first responders to tend to those who cannot self-evacuate. State and local governments are closest to those affected by natural disasters, and have always been the lead in response and recovery. The federal government acts in a supporting role, providing assistance, logistical support, and certain supplies. The Federal government is responsible for meeting those requests from the state – before, during and after the disaster. FEMA and the Department of Homeland Security began preparations for this hurricane season months ago and we continue to refine our processes and become better prepared.

For more information on preparing for emergencies, please visit Ready.gov.

Source: http://www.dhs.gov/xprepresp/editorial_0846.shtm

27. *June 01, Government Technology* — **New online alert system to enhance New York emergency response.** New York Governor Eliot Spitzer announced Thursday, May 31, two important initiatives designed to enhance the state's ability to alert the public in emergency situations and respond after disasters. The first initiative will provide Web-based emergency alerts to the public. The new system — dubbed NY-ALERT — will provide National Weather Service bulletins about severe weather, advisories on road closures, and other emergency response information from federal, state and local authorities. The second initiative — called NY-DELIVERS — will forge public-private partnerships to support the state's emergency response missions. The initiative is modeled on best practices identified after Hurricane Katrina. The two initiatives are expected to be operational within 60 days.

Source: <http://www.govtech.com/gt/articles/123704>

May 30, IDG News Service — **Cell phones to warn of earthquakes in Japan.** Cell phones in Japan could soon provide a vital warning, seconds ahead of a major earthquake. The country's three largest cellular carriers plan to develop a way to automatically funnel alerts to cell phones from a new government advance warning system, which went into operation last year. The system ties together an extensive network of earthquake monitors on a high-speed network to provide data to a variety of users, including TV stations, manufacturers, and cell phone operators. The amount of warning varies and could be anything from a few seconds to up to a minute. The buildings are equipped with receivers to receive data from the government or service providers. The alarm system is designed to automatically stop heavy machinery or save computer data. In the future, it may also be able to automatically shut off gas valves. The cell phone companies hope to have a system launched in 2008.

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9021878&intsrc=news_list

[[Return to top](#)]

Information Technology and Telecommunications Sector

29. *June 01, US-CERT* — Apple releases update for Xserve Lights-Out Management

Firmware. Apple releases Firmware Update 1.0 to address a vulnerability in Xserve Lights-Out Management Firmware. The vulnerability lies in Apple's implementation of IPMI and may allow a remote, unprivileged ipmitool user to gain administrative privileges on a Xserve system.

US-CERT encourages users to apply Firmware Update 1.0 as soon as possible:

<http://docs.info.apple.com/article.html?artnum=305571>

Source: http://www.us-cert.gov/current/index.html#apple_releases_firmware_update_for1

30. *June 01, IDG News Service* — Google Desktop vulnerable to new attack. Just one day after a security researcher showed how Google Inc.'s Firefox toolbar could be exploited in an online attack, a similar flaw has been discovered in the Google Desktop. On Thursday, May 31, a proof of concept was posted showing how attackers could use Google Desktop to launch software that had already been installed on the victim's computer. The attack is hard to pull off and could not necessarily be used to install unauthorized software on the victim's PC. To exploit the Google Desktop vulnerability, an attacker would first have to launch a successful "man-in-the-middle" attack, somehow placing himself between the victim and Google's servers. This could be done by tricking the victim into logging onto a malicious wireless network, said Robert Hansen, a Web security consultant. Once this was done, the hacker could launch the attack by changing the Web pages being delivered to the victim's PC. By returning Web pages that have been doctored with new JavaScript code, the victim could be tricked into clicking onto a malicious link, he said.

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9022561&intsrc=hm_list

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

31. *May 31, Plain Dealer (OH)* — **Ohio dams are showing their age.** Residents around Briar Lake in Solon, OH, want the lake's dam repaired, but the \$1 million cost to preserve what only a few can enjoy has prompted heated debate as city and state officials and homeowners grapple with who will pay. Briar Lake is typical of more than 1,700 dams in the state, and one of 261 in Northeast Ohio, that are showing their age, say Ohio Department of Natural Resources (ODNR) officials. Most are small recreational dams at private developments or at golf courses. Others are large water filtration or retention basins like those at the Shaker Lakes in Shaker Heights, which could cause far more destruction if one were to collapse. "Many of these dams were built before state regulations were imposed in 1963," said Mark Ogden, administrator of dam safety for ODNR. "Many don't meet the standards and are not maintained." There are more than 50,000 dams in Ohio. Most are small and not regulated. But ODNR oversees more than 1,000, including more than 400 that are considered Class 1, or high risk, like Solon's. Catastrophic dam failures of the past led to stringent regulations in place today, Ogden said. In 1990, the Shadyside, OH, dam failed and killed 26 people and destroyed 80 homes.

Source: <http://www.cleveland.com/news/plaindealer/index.ssf?/base/news/1178008427327380.xml&coll=2>

32. *May 30, KXLY (WA)* — **Man arrested with bomb in his pants.** A West Plains, WA, resident was arrested late Wednesday afternoon, May 30, after it was discovered he had a golf ball-sized improvised explosive device in his pants. Lloyd Gable, 51, was booked into the Spokane County Jail on a single felony count of Unlawful Possession of an Explosive Device. Gable lived at the Hilltop Mobile Home Park and the park manager called authorities Wednesday morning to report that he thought Gable was building bombs in his trailer. When deputies arrived they called to Gable to come out of his trailer and when he did asked him about the bombs. Gable confirmed he had one in his pants so they handcuffed him and called in the Explosives Disposal Unit, which removed the golf ball-sized bomb from his pants. Lieutenant Chan Bailey said the device recovered was capable of causing serious bodily harm or death if it had exploded.

Source: http://www.kxly.com/news/?sect_rank=2§ion_id=560&story_id=11486

[[Return to top](#)]

General Sector

Nothing to report.

[[Return to top](#)]

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.